

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 November 2002 (28.11.2002)

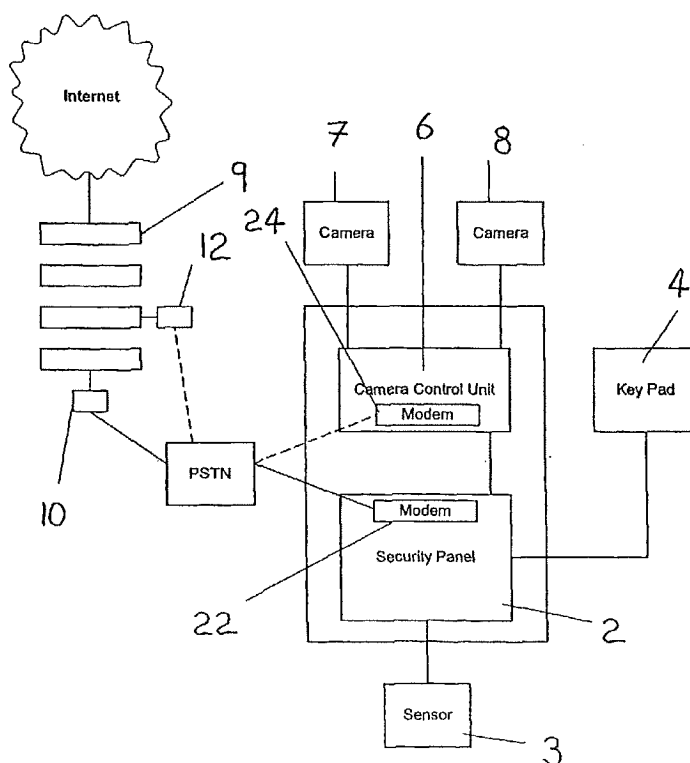
PCT

(10) International Publication Number
WO 02/095702 A1

- (51) International Patent Classification⁷: **G08B 15/00** (74) Agents: **GOODENOUGH, Nigel et al.**; A.A. Thornton & Co, 235 High Holborn, London WC1V 7LE (GB).
- (21) International Application Number: **PCT/GB02/02091**
- (22) International Filing Date: **7 May 2002 (07.05.2002)** (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (30) Priority Data: **0112364.5** **21 May 2001 (21.05.2001)** **GB**
- (71) Applicant (*for all designated States except US*): **INTA-MAC SYSTEMS LIMITED** [GB/GB]; 10 Owl Close, Moulton Park, Northampton NN3 6HZ (GB).
- (72) Inventor; and (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (75) Inventor/Applicant (*for US only*): **MEAGHER, James, Kevin** [GB/GB]; 1 Glebe Farm Court, Great Doddington, Willingborough, Northants NN29 7TP (GB).

[Continued on next page]

(54) Title: **SECURITY SYSTEM**



(57) Abstract: The present invention relates to a security system and method for providing the same. The invention relates particularly, but not exclusively, to domestic security systems for detecting intruders within the home. A security system (20) is provided as comprising a sensor (3) for detecting the occurrence of an unauthorised event; a camera (7,8) for generating data suitable for the production of a picture; and means (24) for sending said data to a remote internet server (9) in response to said sensor (3) detecting the occurrence of an event.

WO 02/095702 A1

WO 02/095702 A1



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

- 1 -

SECURITY SYSTEM

The present invention relates to a security system and method for providing the same. The invention relates particularly, but not exclusively, to domestic security systems for detecting intruders within the home.

It is well known for commercial and domestic properties to be provided with security systems for preventing unauthorised entry and for raising an alarm once an unauthorised entry has occurred. A conventional security system will typically comprise one or more sensors for locating at points of entry of a property (e.g. doors and windows), one or more pressure sensors for locating on a floor of the property, and/or one or more infrared sensors for wall mounting within a property. In this way, a security system can be well equipped to detect an initial unauthorised entry into a property and any subsequent unauthorised movement within a property. A conventional security system will also generally be provided with an audible alarm which may be activated when a sensor detects an unauthorised entry or movement. Interested third parties (e.g. neighbouring property owners) are thereby made aware of an unauthorised entry and the individual giving rise to the alarm is warned off. It is also known for conventional security systems to communicate an alarm to a particular third party (generally the police through an alarm receiving centre) so that appropriate and effective action can be immediately taken. This communication can be provided simultaneously with an audible alarm or as an alternative thereto.

Although the aforementioned prior art security systems are effective at both detecting unauthorised entry to a property and subsequently raising an alarm, such systems can give rise to a number of difficulties. Firstly, it is not uncommon for

- 2 -

sensors to erroneously trigger an alarm where no unauthorised entry or movement has been made. In these circumstances, an audible alarm (if provided) will be undesirably maintained until automatically terminated or manually terminated by a third party. Where an alarm is communicated to a third party obliged to investigate the source of the alarm, an erroneous detection by a sensor can be an inconvenient and costly waste of time. Secondly, conventional security systems rely on third parties rather than the owner of the relevant property to react to an alarm. Regrettably, due to the tendency for sensors to erroneously detect unauthorised entries, third parties tend to be slow in responding to an alarm once raised. Finally, when a conventional security system accurately detects an unauthorised entry to a property and raises an alarm, the intruder will often have vacated the property before any third party investigates. Thus, a conventional security system will generally only indicate entry to a property without offering any assistance in identifying the intruder.

The present invention attempts to address the aforementioned problems associated with prior art security systems.

A first aspect of the present invention provides a security system comprising a sensor for detecting the occurrence of an unauthorised event; a camera for generating data suitable for the production of a picture; and means for sending said data to a remote internet server in response to said sensor detecting the occurrence of an event.

Thus, a security system according to the present invention may be interrogated through use of the internet. When a sensor of the present invention detects the occurrence of an unauthorised event such as a forced entry into a property, a camera focussed on the event location can be used to provide the owner of the property (or a third party) with a view of the property. The property owner or third party may of course obtain this view over the internet from anywhere in the world. The present invention therefore has the advantages of allowing a property owner to remotely investigate the triggering of an alarm. As a result, the property owner does not need to rely on third parties who may have a tendency to react slowly when an alarm is raised. Furthermore, regardless of the property owner's location in the world, a remote investigation of an alarm can be made quickly, conveniently and inexpensively. Accordingly, an audible alarm generated as a result of an erroneous

sensor detection can be manually investigated, albeit from a remote location, in a rapid and time efficient manner. The nuisance to neighbours associated with an audible alarm can therefore be minimised. Also, pictures generated by the present invention can be advantageously stored so as to assist in identifying an intruder.

The security system may further comprise means for recording said data generated by the camera. The recording means may also be adapted to record said data as said data is generated by the camera and to delete said recorded data once a predetermined condition is achieved. The recording means is preferably adapted to not delete said recorded data when said sensor detects the occurrence of an event.

Ideally, the data sending means is adapted to send said recorded data to a remote internet server when said sensor detects the occurrence of an event. The recording means may also be adapted to not delete said data generated by the camera during a predetermined period which follows said sensor detecting an occurrence of an event. The data sending means may be adapted to send, to a remote internet server, said data generated by the camera during a predetermined period following said sensor detecting the occurrence of an event.

The aforementioned predetermined condition may be achieved by the lapsing of a period of five seconds from generation of said recorded data. Also, the aforementioned predetermined period may be ten seconds.

It may be preferable for the data sending means to be adapted so as to send data at a rate sufficient for the production of one still picture per second. The system of the present invention may further comprise said internet server wherein said server is adapted to record said data sent by the data sending means. Also, the camera may be one of a plurality of cameras comprised in the system. It is preferable for means to be provided for permitting one of said plurality of cameras to be selected so that data generated by a selected camera is sent by the data sending means and so that data generated by a not selected camera is not sent by the data sending means.

A second aspect of the present invention provides a method of providing a security system, the method comprising the steps of detecting the occurrence of an unauthorised event by means of a sensor; generating data suitable for the production of a picture by means of a camera; and sending said data through a

remote internet server in response to detecting the occurrence of an unauthorised event.

The method ideally comprises the further step of recording said data. It may also be preferable to provide the yet further step of deleting said recorded data once a predetermined condition is achieved. Ideally, said recorded data is not deleted when, prior to an achievement of said predetermined condition, the occurrence of an unauthorised event is detected. Preferably, said predetermined condition is achieved by the lapsing of a period of five seconds from generation of said recorded data.

It is further preferable for said recorded data to be sent to a remote internet server when an unauthorised event is detected.

Furthermore, it is preferable for said data generated during a predetermined period following said detecting of an unauthorised event to be not deleted. It is also preferable for said data generated during a predetermined period following said detecting of an unauthorised event to be sent to a remote internet server. Ideally, said predetermined period is ten seconds. Also, said data may be generated at a rate sufficient for the production of one still picture per second.

An embodiment of the present invention will now be described with reference to the accompanying drawings, in which:

FIGURE 1 is a schematic view of a security system according to the present invention; and

FIGURE 2 is a schematic view of a further security system according to the present invention.

The security system 1 shown in the accompanying Figure 1 comprises a security panel 2, a sensor 3 and a keypad 4. The security panel 2, sensor 3 and keypad 4 are commonly found in conventional security systems. In the present embodiment, the sensor 3 is a conventional infrared sensor for sensing movement. The security panel 2 operates to control activation of the sensor 3 and to interpret signals received from said sensor 3. The keypad 4 allows a user to provide the security panel 2 with various instructions. In this latter regard, the keypad 4 may be used to activate or deactivate the sensor 3. In an alternative embodiment, a security system according to the present invention may be provided with more than one sensor and, in such an embodiment, the keypad 4 may be operated by a user so as to activate one or more of

the available sensors. A user may, for example, use the keypad 4 to activate point of entry sensors whilst deactivating infrared sensors for detecting motion. In this way, a user may protect a property whilst allowing movement by persons or pets within the property. This technology is well known and understood by those skilled in the art.

The security system 1 further comprises a modem 5, a camera control unit 6 (an Interactive Control Box - ICBox), and two cameras 7,8. The two cameras 7,8 are CCD web cameras linked to the modem 5 via the camera control unit 6. The security panel 2 is also connected to the modem 5. A retrofitting of the modem 5, camera control unit 6 and cameras 7,8 to a conventional security panel may therefore require modification to said panel so as to permit the aforementioned modem connection. The connection may be made using a four wire serial interface. In this regard, the security panel may be provided with an RS232 port. The modem 5 allows communication between the camera control unit 6 and/or the security panel 2 and a remote internet server 9 via a PSTN line and a receiving unit 10. The receiver unit 10 functions to interpret the alarm protocols used by the security panel 2. Where the receiver unit 10 is to be provided as part of a retrofit package, said unit 10 is programmed to interpret the standard alarm protocols of existing security panels. The receiver unit 10 translates the alarm protocols of an associated security panel into a standard format which can be understood by the server 9 and presented to a property owner (or an authorised third party).

In a modification to the security system 1 shown in Figure 1, a further security system 20 is shown in Figure 2 of the accompanying drawings wherein the single modem 5 is replaced with two separate dedicated modems 22,24. The first modem 22 is dedicated to the security panel 2 and allows communication of standard alarm protocol signals to the remote internet server 9 via a PSTN line connection and a receiving unit 10. In this regard, the modified security system 20 operates in a similar manner to the security system 1 shown in Figure 1. Also, as in the case of the security system 1 of Figure 1, a retrofitting of the security panel modem 22 may require modification to the security panel 2. Connection of the modem 22 to the security panel 2 may be made using a four wire serial interface. This may be achieved through use of an RS232 port provided in the security panel 2. The second modem 24 is dedicated to the camera control unit 6 and operates to communicate digital images

from the cameras 7,8 to the remote internet server 9 via a PSTN line connection and a receiving unit 12. The receiving unit 12 places the received signal in a format suitable for the internet server 9. Communication between the security panel 2 and the camera control unit 6 is achieved either by means of a direct link or by means of an indirect link via one or both of the modems 22,24.

In both security systems 1,20 shown in the accompanying drawings, the cameras 7,8 are black and white web cameras which are strategically located inside or outside a property and are preferably focussed on the detection area associated with the sensor 3. A security system according to the present invention having more than a single sensor will be preferably provided with at least one camera for each sensor. The or each camera associated with a particular sensor will be focussed on the area or point of entry protected by the sensor. A camera associated with an infrared sensor will, for example show a wide angle view of the area in which the sensor is capable of detecting movement.

The cameras 7,8 in the present embodiments are capable of generating grey scale pictures. Alternative cameras may however be provided for generating colour pictures or for operating in low light conditions.

The cameras 7,8 are each powered through the security panel 2 via the camera control unit 6. When the security system 1 is activated, the camera control unit 6 records images generated by the two cameras 7,8. In an embodiment comprising more than one sensor 3, the camera control unit 6 will only record images generated by those cameras associated with a sensor which has been activated. The camera control unit 6 is capable of processing images generated by a total of eight cameras and communicates with said cameras via high-speed serial links. Due to processing and memory constraints, the camera control unit 6 records images generated by each camera 7,8 at a rate of one picture per second. Again, due to memory constraints, each picture recorded by the camera control unit 6 is retained for a finite period of time. The camera control unit 6 has sufficient memory to allow five pictures from up to eight cameras to be stored. Thus, a recordal rate of one picture per second, images from a particular camera will be retained for a period of five seconds.

The control logic of the camera control unit 6 is such that, upon detection by the sensor 3 of a suspected unauthorised event (i.e. an unauthorised entry

- 7 -

into a property), the images previously generated by the cameras 7,8 associated with the sensor 3 and presently stored within the memory of the camera control unit 6 are downloaded via the associated modem (i.e. modem 5 for the security system 1 of Figure 1 and modem 24 for the security system 20 of Figure 2) to the internet server 9. In this way, images of a protected area of property immediately prior to sensor detection are made available.

The control logic of the camera control unit 6 is also such that images generated in a finite period after a sensor detection are sent downline to the internet server 9. Thus, in the present embodiment, when the sensor 3 detects an unauthorised movement, images generated by the cameras 7,8 in the subsequent predetermined period are downloaded to the internet server 9. In the present embodiment, said predetermined period is ten seconds. Accordingly, images of a property in a period of five seconds prior to a sensor detection and a period of ten seconds after a sensor detection are available for remote viewing by the property owner (or an authorised third party) by means of the internet.

The image data generated by each camera 7,8 is transmitted to the internet server 9 in a compressed format. Once received by the internet server 9, the image data may be processed so as to provide photographic pictures. This processing may occur automatically as soon as the image data is received by the internet server 9 or may occur in response to the internet server 9 being interrogated by the property owner or other authorised party. Also, in addition to the aforementioned image data being transmitted to the internet server 9, said data may be permanently retained within the memory of the camera control unit 6 until cleared by the property owner.

When the internet server 9 receives (via receiver unit 10) image data from the camera control unit 6 as a result of the sensor 3 detecting an unauthorised event, the server 9 automatically sends a message to the property owner (an authorised third party) by means of e-mail, voicemail or SMS. A message may also be sent to a third generation mobile device. Other communication means may also be used. The message receiver is thereby notified of a potential unauthorised event associated with a particular property. The message receiver may then access (by means of the internet server 9) pictures of the property which were recorded in the five second period before the unauthorised event and the ten second period after the unauthorised event.

- 8 -

The internet server 9 not only presents images of a property, but also presents other information regarding the status of the security system 1,20 and the associated property. Such other information may, for example, include identification of the sensor detecting an unauthorised event, the number of times said sensor has been triggered and/or a time and date stamp on each picture (or video frame) so as to provide accurate time evidence of an unauthorised event.

As well as transmitting data to the internet server 9, the camera control unit 6 is provided with control logic allowing the reception and interpretation of instructions provided by the internet server 9. The camera control unit 6 may, for example, allow live remote viewing of a property via the internet server 9. Thus, once the sensor 3 has detected an unauthorised event and the recorded images have been viewed, a property owner may then view live images generated by the cameras 7,8 so as to determine current status at the property. The camera control unit 6 may also allow the field of view of a particular camera 7,8 to be adjusted, permit specific sensors to be activated or deactivated, and/or allow the length of the aforementioned recording periods (i.e. the five and ten second periods) to be altered. Indeed, the camera control unit 6 may be provided with suitable control logic for allowing complete remote control of the security system 1,20 by means of the internet server 9.

The present invention is not limited to the specific embodiments and methods described above. Alternative arrangements will be apparent to a reader skilled in the art. For example, one or more microphones may be provided so that sound, as well as images, can be recorded and listened to from a remote location. Furthermore, the transmission/processing rates may be increased so as to improve picture/video quality. The camera control unit 6 may also be provided as an integral part of the security panel 2. The camera control unit 6 and the security panel 2 may have a common power input line.

CLAIMS:

1. A security system comprising a sensor for detecting the occurrence of an unauthorised event; a camera for generating data suitable for the production of a picture; and means for sending said data to a remote internet server in response to said sensor detecting the occurrence of an event.
2. A security system as claimed in claim 1, the system further comprising means for recording said data generated by the camera.
3. A security system as claimed in claim 2, wherein the recording means is adapted to record said data as said data is generated by the camera and to delete said recorded data once a predetermined condition is achieved.
4. A security system as claimed in claim 3, wherein the recording means is adapted to not delete said recorded data when said sensor detects the occurrence of an event.
5. A security system as claimed in claim 3 or 4, wherein the data sending means is adapted to send said recorded data to a remote internet server when said sensor detects the occurrence of an event.
6. A security system as claimed in any of claims 3 to 5, wherein the recording means is adapted to not delete said data generated by the camera during a predetermined period which follows said sensor detecting the occurrence of an event.
7. A security system as claimed in any of claims 3 to 6, wherein the data sending means is adapted to send, to a remote internet server, said data generated by the camera during a predetermined period following said sensor detecting the occurrence of an event.

- 10 -

8. A security system as claimed in claim 6 or 7, wherein said predetermined period is ten seconds.
9. A security system as claimed in any of claims 3 to 8, wherein said predetermined condition is achieved by the lapsing of a period of five seconds from generation of said recorded data.
10. A security system as claimed in any preceding claim, wherein the data sending means is adapted to send data at a rate sufficient for the production of one still picture per second.
11. A security system as claimed in any preceding claim, the system further comprising said internet server wherein said server is adapted to record said data sent by the data sending means.
12. A security system as claimed in any preceding claim, wherein said camera is one of a plurality of cameras comprised in the system.
13. A security system as claimed in claim 12, wherein means are provided for permitting one of said plurality of cameras to be selected so that data generated by a selected camera is sent by the data sending means and data generated by a not selected camera is not sent by the data sending means.
14. A method of providing a security system, the method comprising the steps of detecting the occurrence of an unauthorised event by means of a sensor; generating data suitable for the production of a picture by means of a camera; and sending said data to a remote internet server in response to detecting the occurrence of an unauthorised event.
15. A method as claimed in claim 14, the method comprising the further step of recording said data.

- 11 -

16. A method as claimed in claim 15, the method comprising the further step of deleting said recorded data once a predetermined condition is achieved.
17. A method as claimed in claim 16, wherein said recorded data is not deleted when, prior to an achievement of said predetermined condition, the occurrence of an unauthorised event is detected.
18. A method as claimed in claim 16 or 17, wherein said predetermined condition is achieved by the lapsing of a period of five seconds from generation of said recorded data.
19. A method as claimed in any of claims 16 to 18, wherein said recorded data is sent to a remote internet server when an unauthorised event is detected.
20. A method as claimed in any of claims 16 to 19, wherein said data generated during a predetermined period following said detecting of an unauthorised event is not deleted.
21. A method as claimed in any of claims 16 to 19, wherein said data generated during a predetermined period following said detecting of an unauthorised event is sent to a remote internet server.
22. A method as claimed in claim 20 or 21, wherein said predetermined period is ten second.

1/2

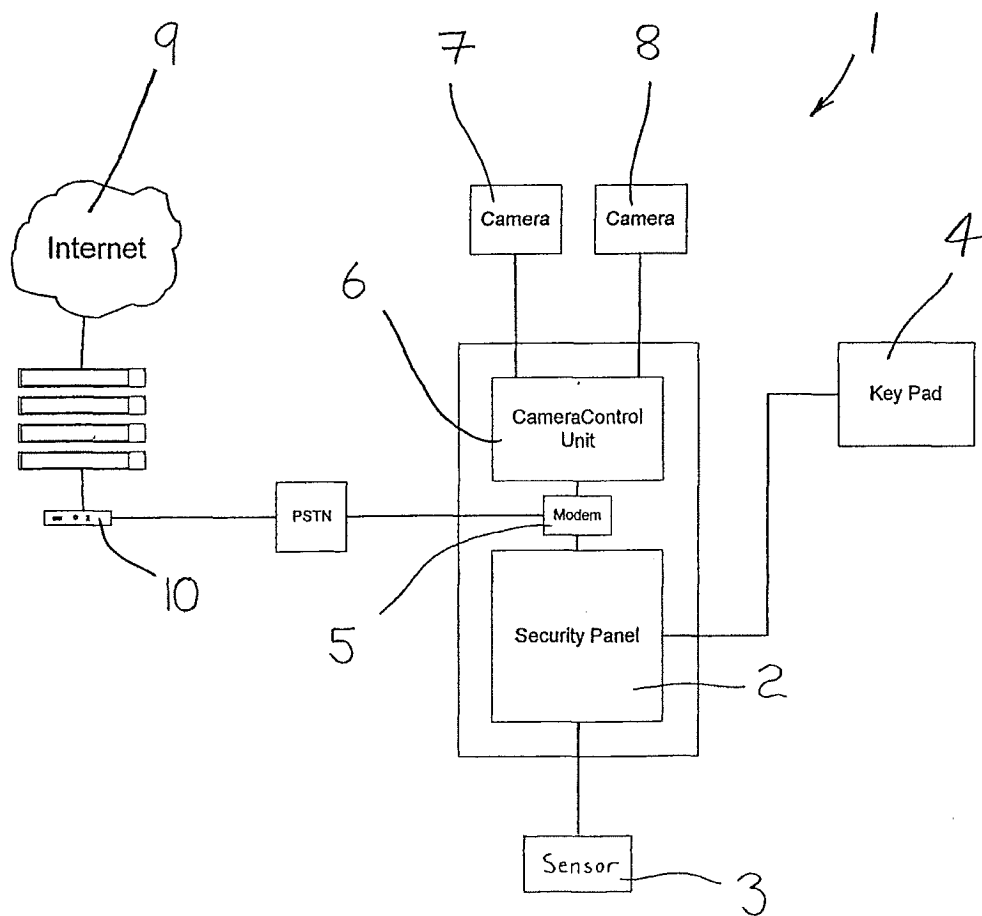


FIG. 1

2/2

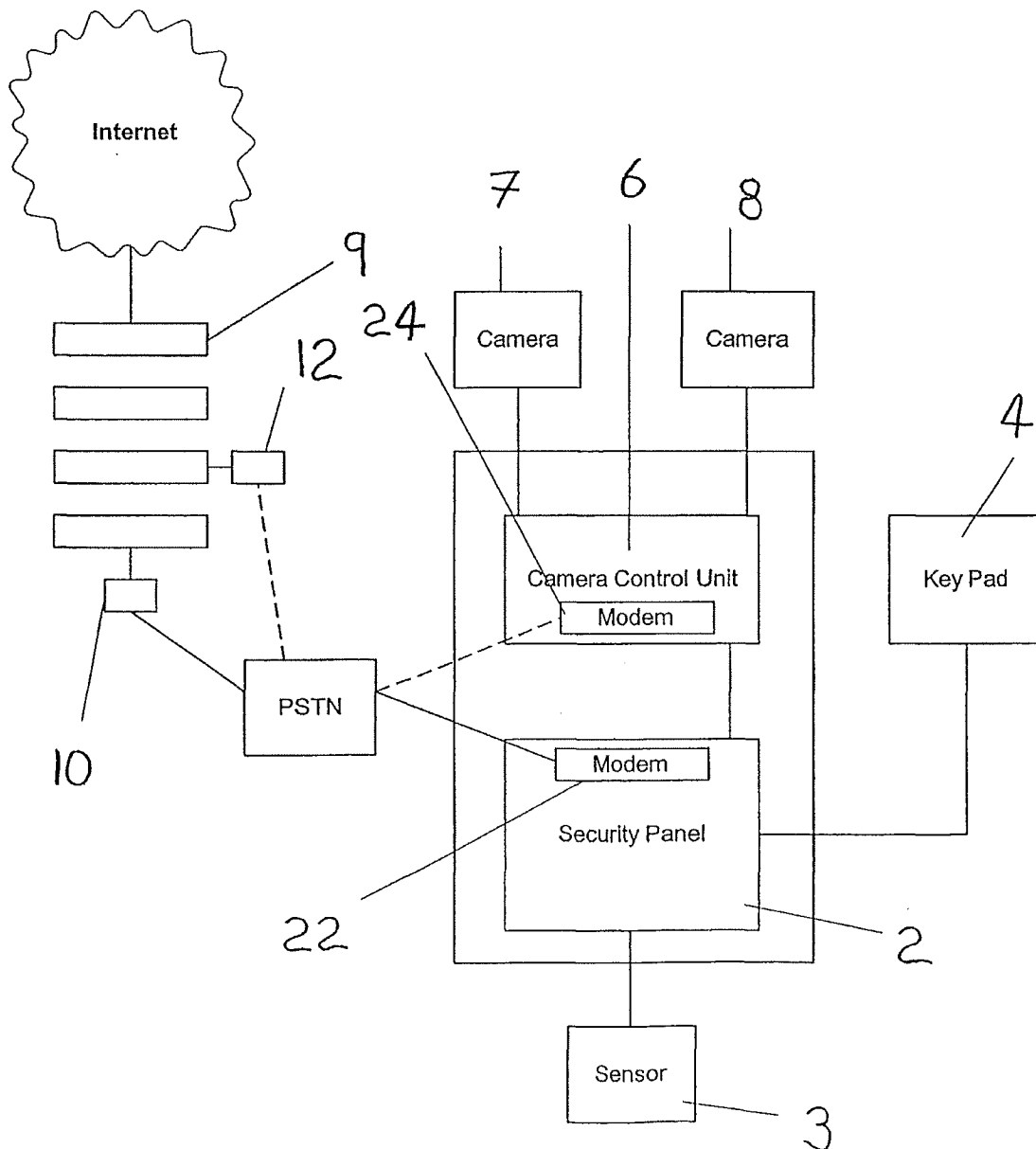


FIG. 2

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 02/02091

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G08B15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G08B H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 27864 A (BELL ADDISON ;BELL DERYL L (US); KRAFT BRADY NEIL (US)) 12 September 1996 (1996-09-12) abstract	1-22
X	FR 2 707 029 A (PROVENCE ALPES CORSE CAISSE EP ;ELECTRE SARL; ELECTRE SARL) 30 December 1994 (1994-12-30) abstract	1-22
A	EP 0 944 260 A (TOKYO SHIBAURA ELECTRIC CO) 22 September 1999 (1999-09-22) abstract	1
A	DE 198 55 154 A (BUNGE MICHAEL ;HAART CHRISTIAN (DE)) 8 June 2000 (2000-06-08) claims 1-4	1

☐ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

23 August 2002

Date of mailing of the international search report

03/09/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sgura, S

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 02/02091

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9627864	A	12-09-1996	AT 206548 T	15-10-2001
			CA 2248069 A1	12-09-1996
			DE 69615713 D1	08-11-2001
			DK 898770 T3	21-01-2002
			EP 0898770 A1	03-03-1999
			ES 2167551 T3	16-05-2002
			PT 898770 T	28-02-2002
			WO 9627864 A1	12-09-1996
FR 2707029	A	30-12-1994	FR 2707029 A1	30-12-1994
EP 0944260	A	22-09-1999	JP 11266487 A	28-09-1999
			EP 0944260 A2	22-09-1999
			US 6239833 B1	29-05-2001
DE 19855154	A	08-06-2000	DE 19855154 A1	08-06-2000